BITSIGHT®

Managing Vendor Risks

State of North Carolina
2019 Annual Cyber Awareness Symposium

www.bitsight.com

Agenda

Vendor risk management is a key aspect of IT operations. Every organization should have processes in place to carefully assess and identify issues when considering using outsourced services.

- The challenges with current TPRM programs
- The art of the possible--what a perfect program might look like
- Data-centric assessments
- A day in the life of a risk analyst
- Whiteboard session--challenges, goals, dashboards
- Components of a solid TPRM program
- Optimizations to current operations

BITSIGHT®

The Trouble with Third-Parties

Huge Spend on Digital Transformation; Cybersecurity Spend Not Aligned

Organizations are undergoing digital transformation to better deliver products and services to customers and drive innovation...

40% of all technology spending will go toward digital transformations*

$2T the amount enterprises will spend on digital transformations by 2019*

*Source: IDC

NEW INITIATIVES TO DRIVE INNOVATION

CLOUD

IoT

MOBILE

79% of organizations are adopting new technologies at a rate faster than they can address new security issues (Accenture)

Digital Transformation Expands Attack Surface

Companies continue to expand their digital ecosystem….

70% *of organizations have "moderate" to "high" dependency on external organizations* [1]

...Which poses new risks to the business

83% *of organizations have experienced a third-party incident in the last three years* [2]

[1] Results from 2019 Deloitte survey
[2] Deloitte - EERM 2019 Survey

Risk is Growing, Actions Not Taken

65% *rate their TPRM program as less than highly effective*

64% *of large organizations have no visibility into their third party environments*

54% *of organizations do not monitor the security and privacy practices of vendors*

"2019 may be the year the Supply Chain Ecosystem, and **concern about third party risk, officially hits the tipping point**…"

- Kirstjen Nielson, Secretary of US Homeland Security @ RSA Conference 2018

Increased Regulatory Focus

GDPR

DFAR

FFIEC

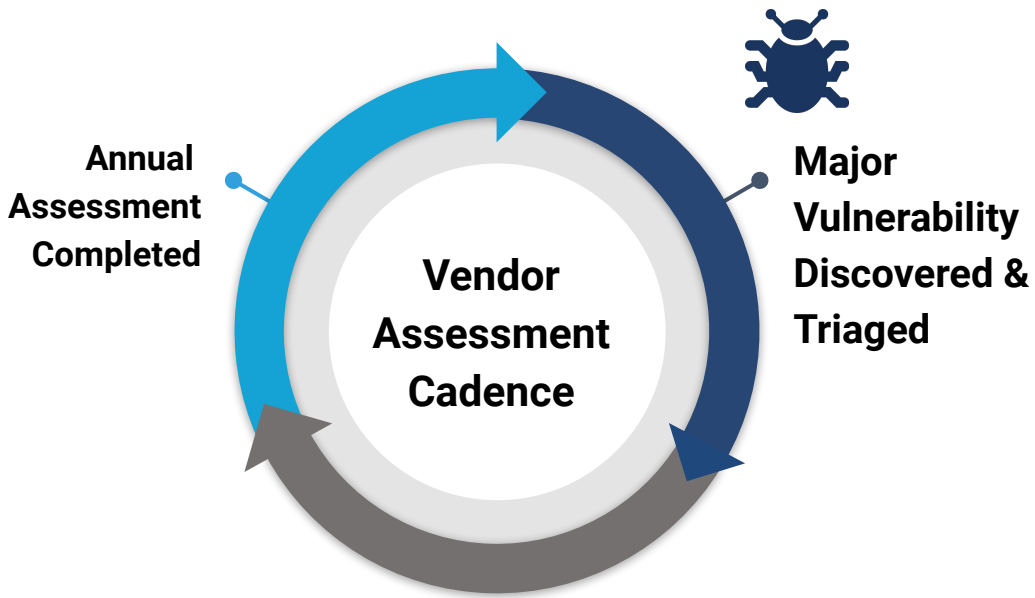
NIST

Hong Kong Monetary Authority

Lack of Confidence in Current Approaches

Existing Processes

- Questionnaires
- Onsite assessments
- Penetration tests



No visibility on impact or potential risk until next assessment

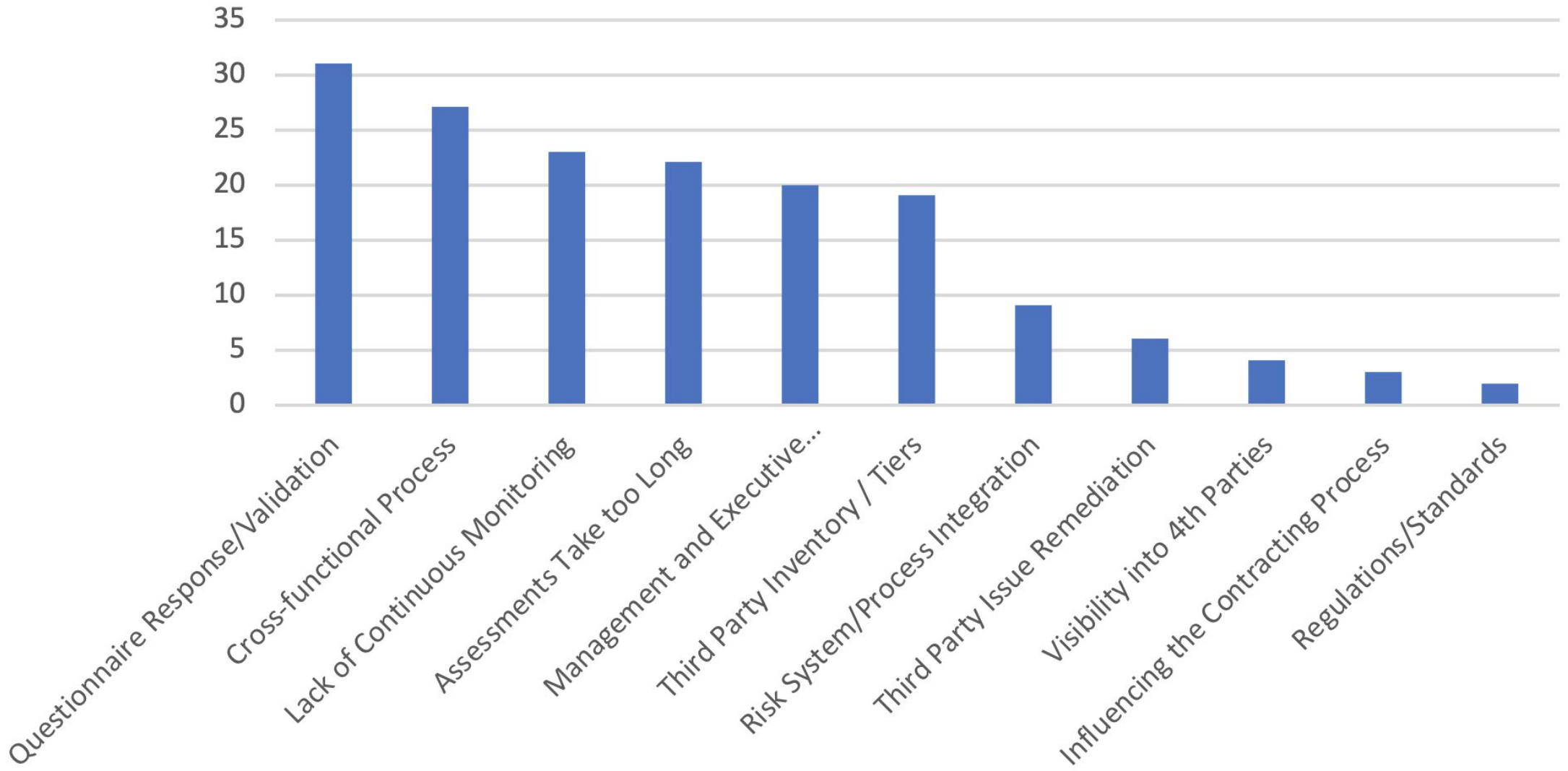
"I know all the risk **based on what my vendors tell me**"

"A **single point-in-time** view of risk is good enough"

"I only need to **focus on my top tier vendors** - the others don't matter"

Current processes are valuable efforts to understand third party cyber risk but are not continuous, scalable, and staying ahead of this dynamic risk

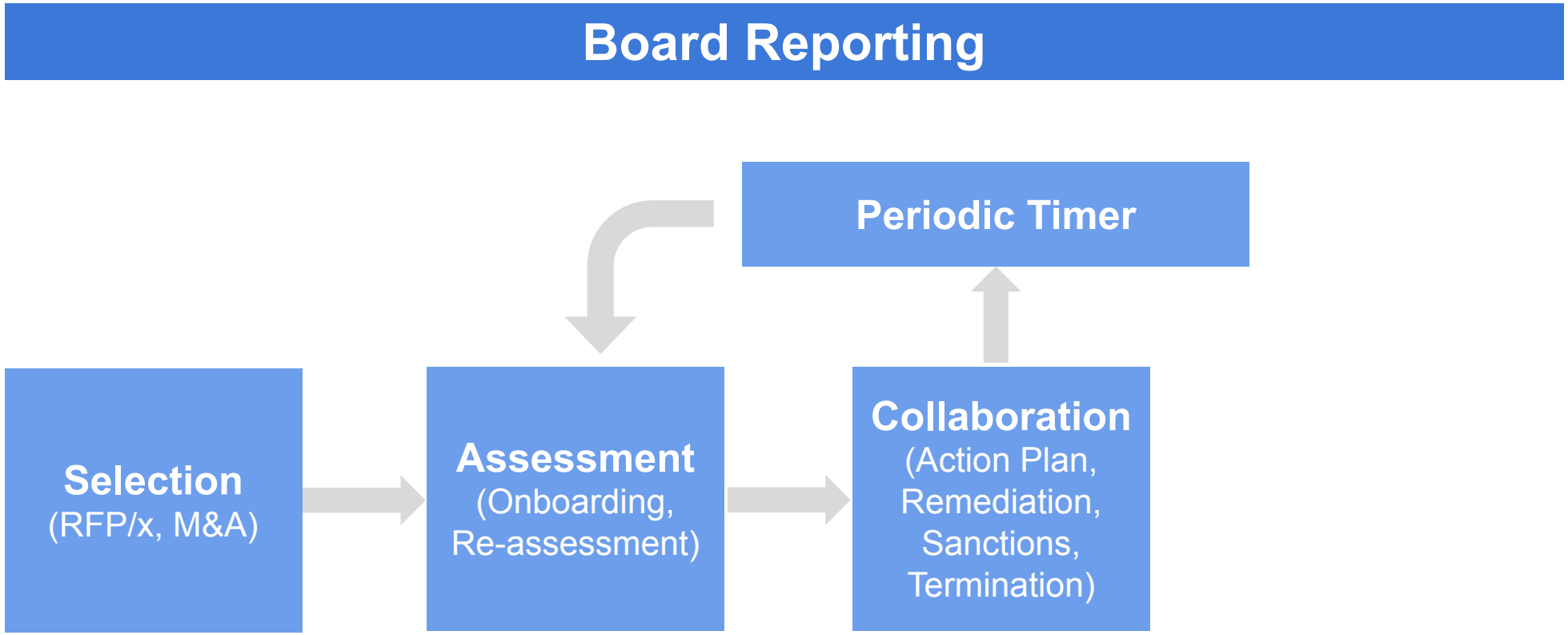
Greatest Challenges



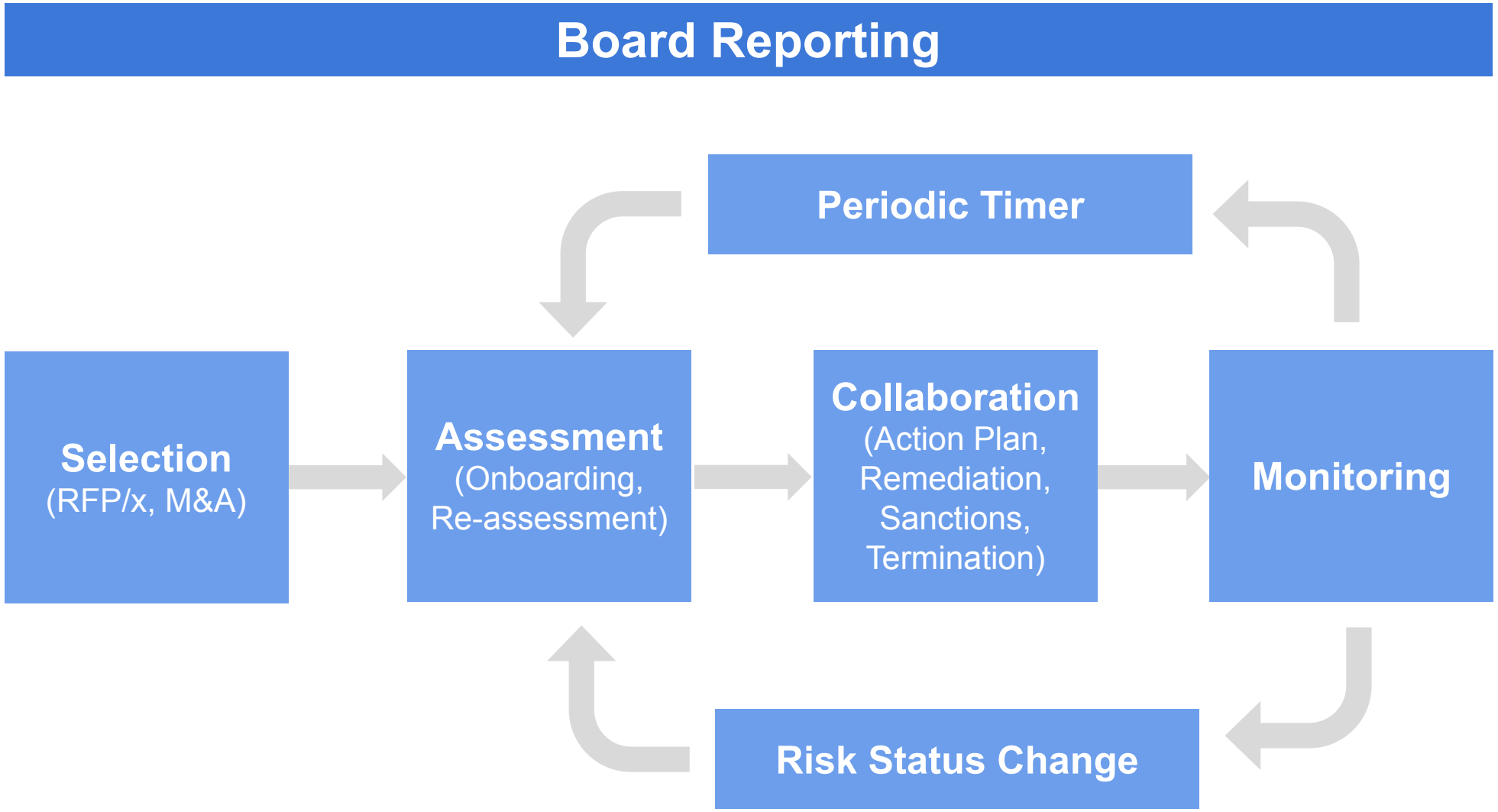
BITSIGHT®

TPRM 2.0

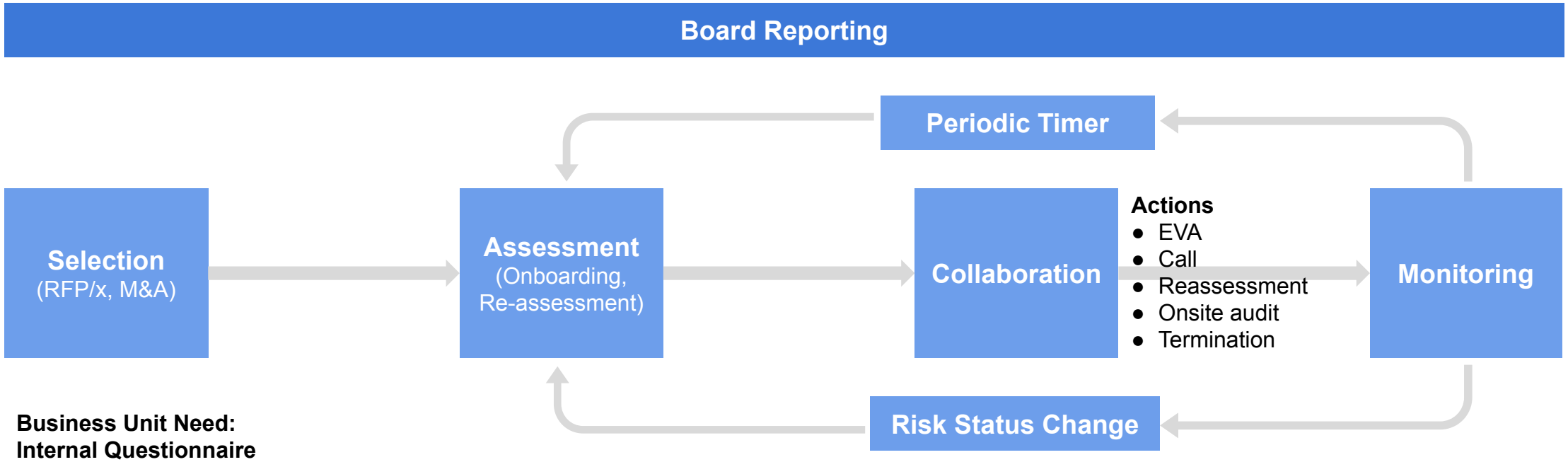
Legacy TPRM Workflow



Continuous TPRM Workflow



Continuous TPRM Workflow



Business Unit Need: Internal Questionnaire (inherent risk)

- Data sensitivity
- Systems access
- Business dependency
- Geographic reach

→ **Tiering**

Types of Security Program Evidence

- Questionnaire Responses (& artifacts)
- Certifications (ISO, SOC2, other audit)
- BitSight headline rating and risk vectors

Contract Terms

- Will monitor with SRS/BitSight
- Require interaction for observations
- Minimum standards
- Compel to work with BitSight on context

Workflow

- GRC
- Shared questionnaires
- EVA language
- etc.

Third Party Lifecycle

INTEGRATION TO RISK SYSTEMS AND PROCESSES

- GRC – leading indicators
- Issue Management
- Activity Plans
- API Integrations

EVALUATION OF NEW VENDORS

- Verification/Validation
- Evaluate Control Effectiveness

FOCUS ON KEY VENDORS

- Tiering by Criticality
- Recent incidents
- Trending down
- Drive 3 year resource plan
- Validate questionnaires
- Higher quality, data driven conversations

OPERATIONS

- Differentiated Alerting by Tier
- Management by exception
- Remediation and Enable Vendor Access

INVESTIGATION

- Celebrity Vulnerability e.g. ‘Bluekeep’
- 3rd and 4th party investigations

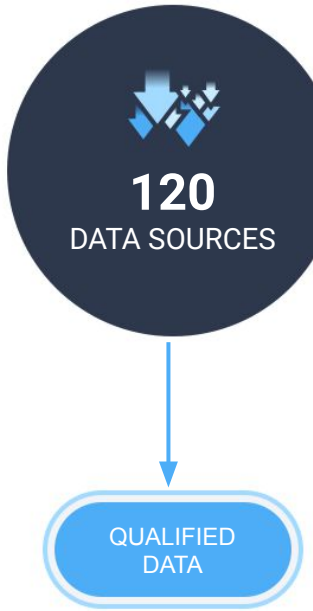
BITSIGHT®

Data-Centric Risk Assessments

How BitSight Security Ratings are Calculated

Collect Data

200+ Billion events daily
Externally observable
World's largest sinkhole



BitSight Data Collection

Over 120+ data feeds

Including proprietary and exclusive data sources

The largest amount of proprietary data collection

BitSight collects 200+ Billion Events on a daily basis across 23 unique risk vectors

Exclusive data partnerships giving unprecedented visibility unavailable elsewhere

BitSight works with major ad networks, service providers and other unique data partners to provide visibility into organizational security posture unavailable elsewhere on the market.

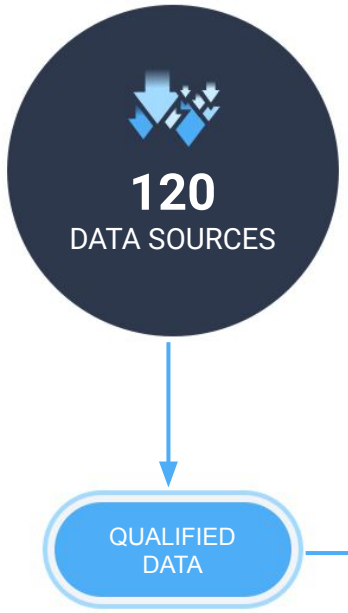
Broadest Visibility into Emerging Areas of Cyber Risk

BitSight has visibility into emerging areas of cyber risk including Mobile Applications, Mobile Software, Internet of Things (IoT), File Sharing and more.

How BitSight Security Ratings are Calculated

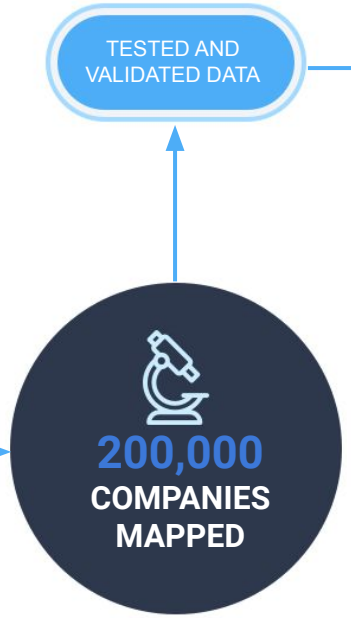
Collect Data

200+ Billion events daily
Externally observable
World's largest sinkhole



Research & Assign

Automated & human validated
Public Internet registries
12+ month history for all companies



BitSight Digital Footprint Curation

Advanced Automated Mapping

Team of over 60+ technical researchers worldwide curating organizational digital footprints

Broad Array of Sources

BitSight uses public registries, corporate documents, and technical methods to determine the IP and domain footprint belonging to a company

Parent-Child Relationship Mapping

BitSight is the only security ratings provider with extensive parent-child relationship mapping to ensure that corporate structure is properly identified

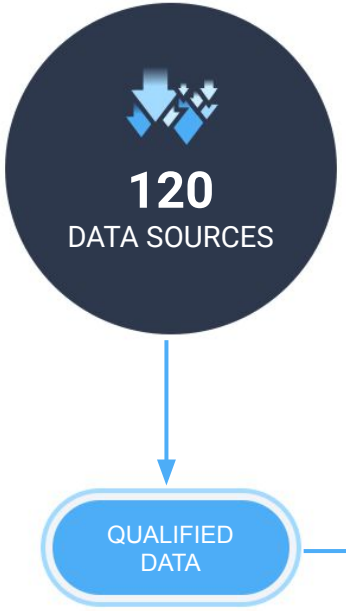
Customizable Mappings of Your Organization

BitSight enables organizations to self-publish relevant ratings to the BitSight platform for better risk visibility and communication. Examples include regional breakouts (e.g. "France Operations"), excluding irrelevant infrastructure like Guest Wifi (e.g. "Corporate Rating") and more.

How BitSight Security Ratings are Calculated

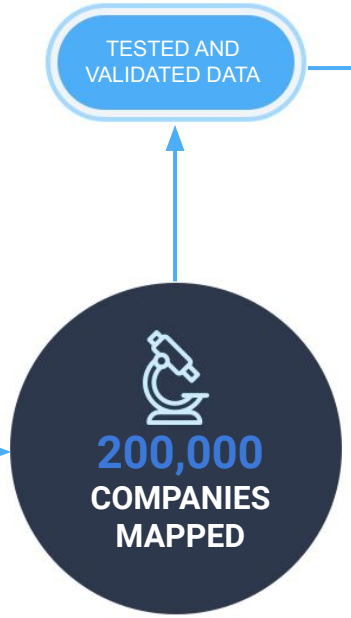
Collect Data

200+ Billion events daily
Externally observable
World's largest sinkhole



Research & Assign

Automated & human validated
Public Internet registries
12+ month history for all companies



Filter & Process

55% Compromised Systems
35% Diligence Information
10% User Behavior
Breaches when applicable

23 Risk Vectors

55% Compromised Systems
Botnet Infections
Spam Propagation
Malware Servers
Unsolicited Comms
Potentially Exploited

35% Diligence Information
SPF Domains
DKIM Records
SSL Certs/Config
Open Ports
Web Application Headers
Patching Cadence
Insecure Systems
Server Software
Desktop Software
Mobile Software
DNSSEC
Mobile Application Security
Domain Squatting

10% User Behavior
File Sharing

Breaches if Applicable

How BitSight security ratings are calculated

Collect Data

200+ Billion events daily
Externally observable
World's largest sinkhole

120
DATA SOURCES

QUALIFIED DATA

Research & Assign

Automated & human validated
Public Internet registries
12+ month history for all companies

TESTED AND VALIDATED DATA

200,000+
COMPANIES MAPPED

Filter & Process

55% Compromised Systems
35% Diligence Information
10% User Behavior
Breaches when applicable

23 RISK VECTORS

PROCESSED DATA

Calculate Rating

Daily Ratings
Range from 250 to 900

Low ratings correlated to higher likelihood of breach

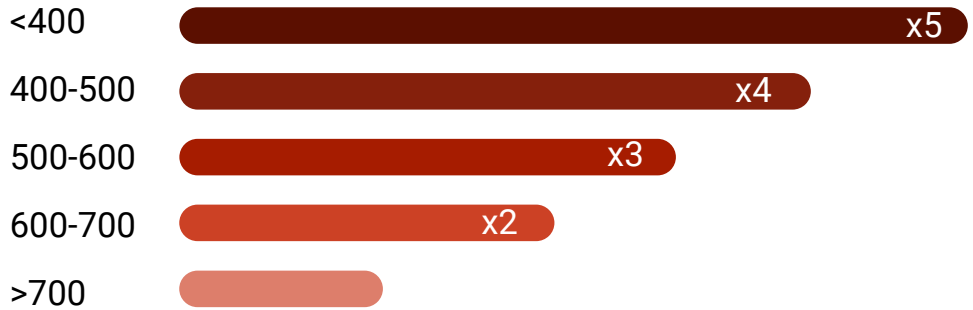
SECURITY RATING

Strong, validated correlation to data breach

BitSight provides a **measurable range of risk** and is the only ratings solution with a **third party verified correlation to breaches**.

Likelihood of suffering a data breach

5x If the security rating drops below 400 as compared to an organization with a 700 or higher*



3x If 50% of computers run outdated Operating System versions**

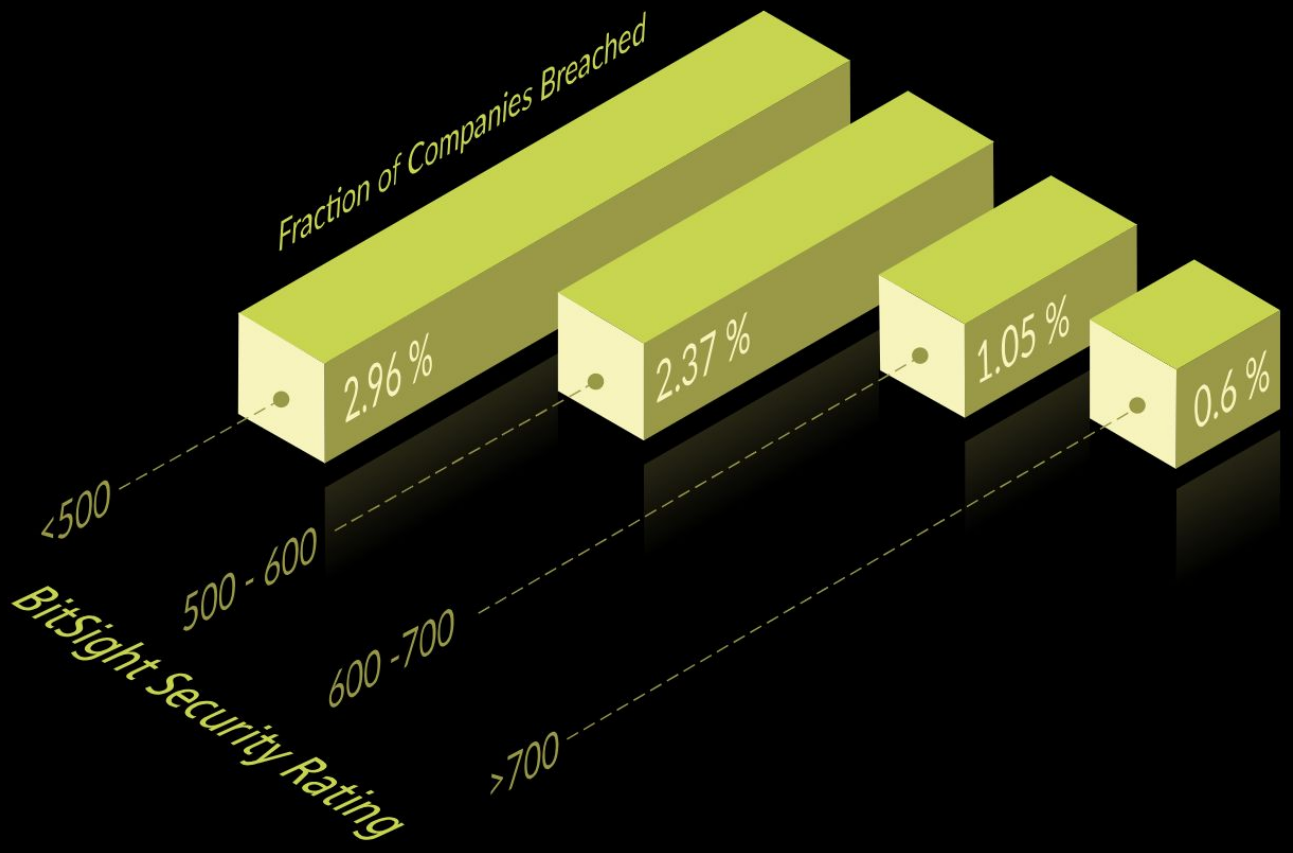
2x If the Botnet Grade is **B or lower*** or the File Sharing grade is **B or lower** or the Open Ports grade is **F**

*AIR Worldwide reviewed and approved our data and analyses

** A Growing Risk Ignored: Critical Updates

*** Beware the Botnets: Botnets correlated to a higher Likelihood of a Significant Breach

A WEALTH OF DATA IS DRIVING NEW INSIGHTS



The insurance industry is gaining real-time insight into which companies are most vulnerable to cyber attacks—insight that can fuel intelligent growth.

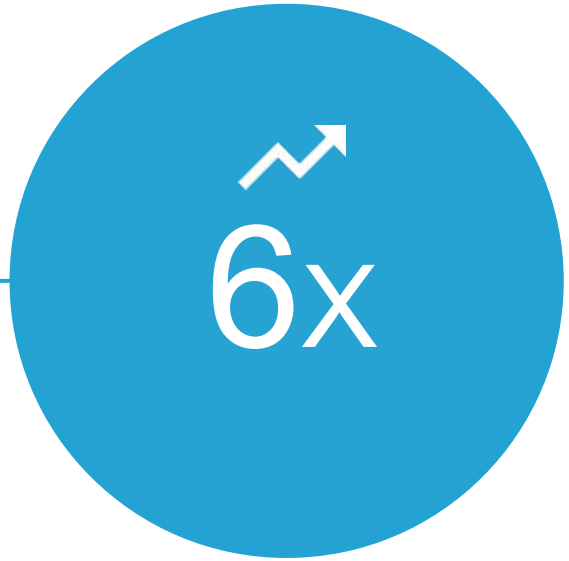
Third Party Monitoring Produces Measurable Results at Scale for TransUnion

Goal: Monitor the information security disposition of critical third party service providers

Actions by BitSight

- Monitor thousands of third parties
- Evaluate risk rating for each provider
- Determine risk areas for action

Results



Third party expansion coverage
with same FT employees

Impactful Results from Vendor Collaboration

Onboarded **496** suppliers and engaged with BitSight Security Ratings as part of this process

56%

Saw a Rating Increase

276

50

Average points increased across this group

*Suppliers on-boarded between May 1st and October 31. Ratings compared between May 1st and Dec 4th

BITSIGHT®

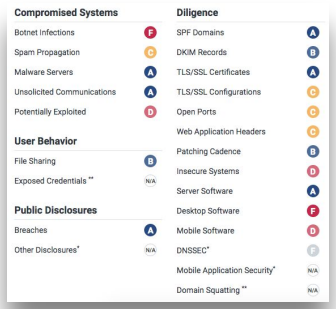
A Day in the Life of a Risk Analyst

The TPRM Maturity Continuum

Visibility

CUSTOMIZE ALERTS

DRILL DOWN ON CRITICAL RISKS



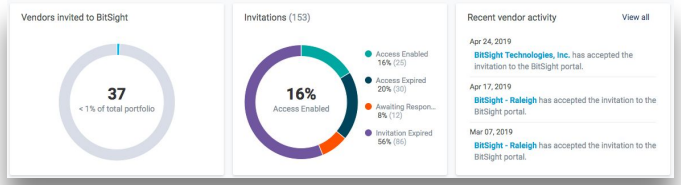
Prioritization

TARGET RESOURCES

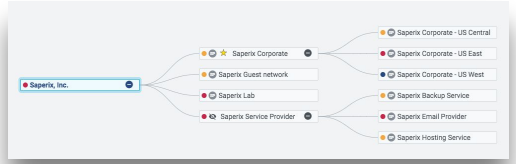
FOCUS ON THE RISKIEST ISSUES

Collaboration

COMMUNICATE PROACTIVELY



TAKE ACTION BASED ON CONTEXT



Messaging to Management / Executive Dashboards

Self

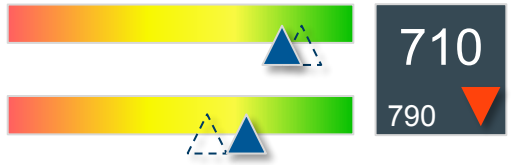
Executive Summary

- Prior to June 2018, at top of Industry Range
- 80 point drop due to configuration of external systems
- Can recover all points quickly

Operational Excellence

Incidents — System compromises & data exposure

Diligence — Configuration, patching, & hardening



710

790

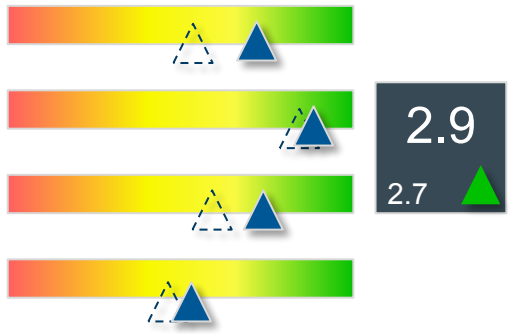
Program Maturity

Identify — Situational awareness: assets, policies

Protect — Defensive controls and procedures

Detect — Automated and manual analysis of data

Respond — Mitigate technical and brand damage



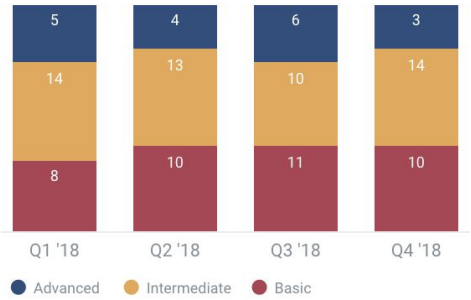
2.9

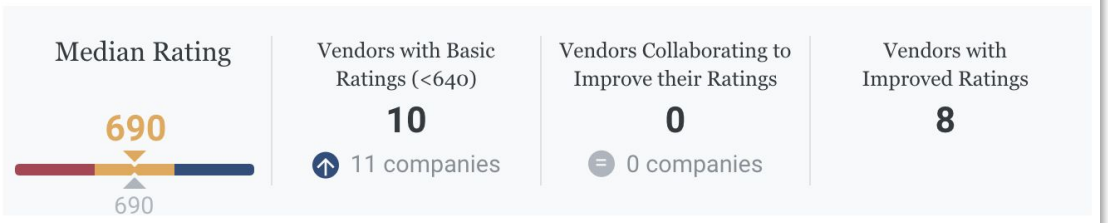
2.7

Vendors

Executive Summary

- Vendors range from 480 to 760
- 1 public compromise, Acme PII exposed
- Reassess 3 vendors (partial / contextual)





Whiteboard Session

What are the challenges with your TPRM program?

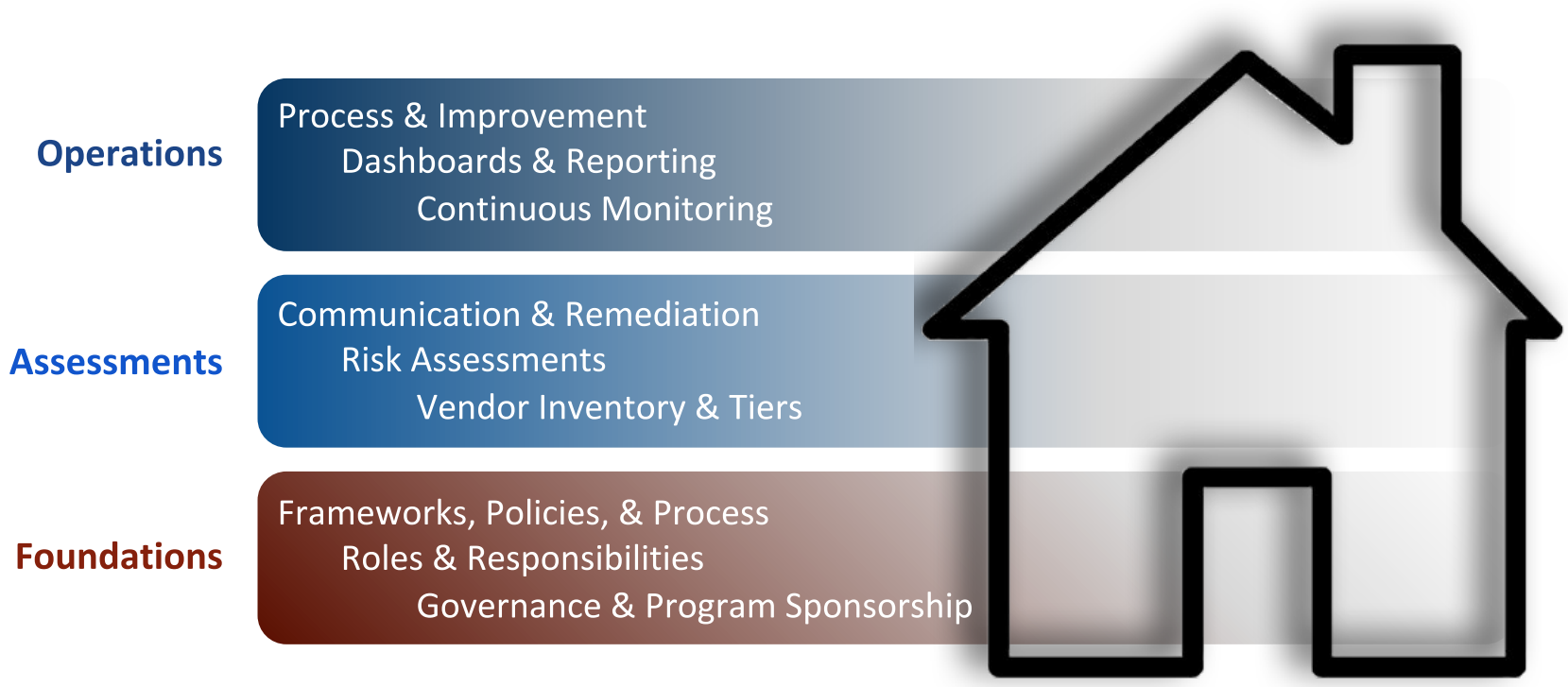
What are you TPRM program goals?

What would be on your ideal executive dashboard?

BITSIGHT®

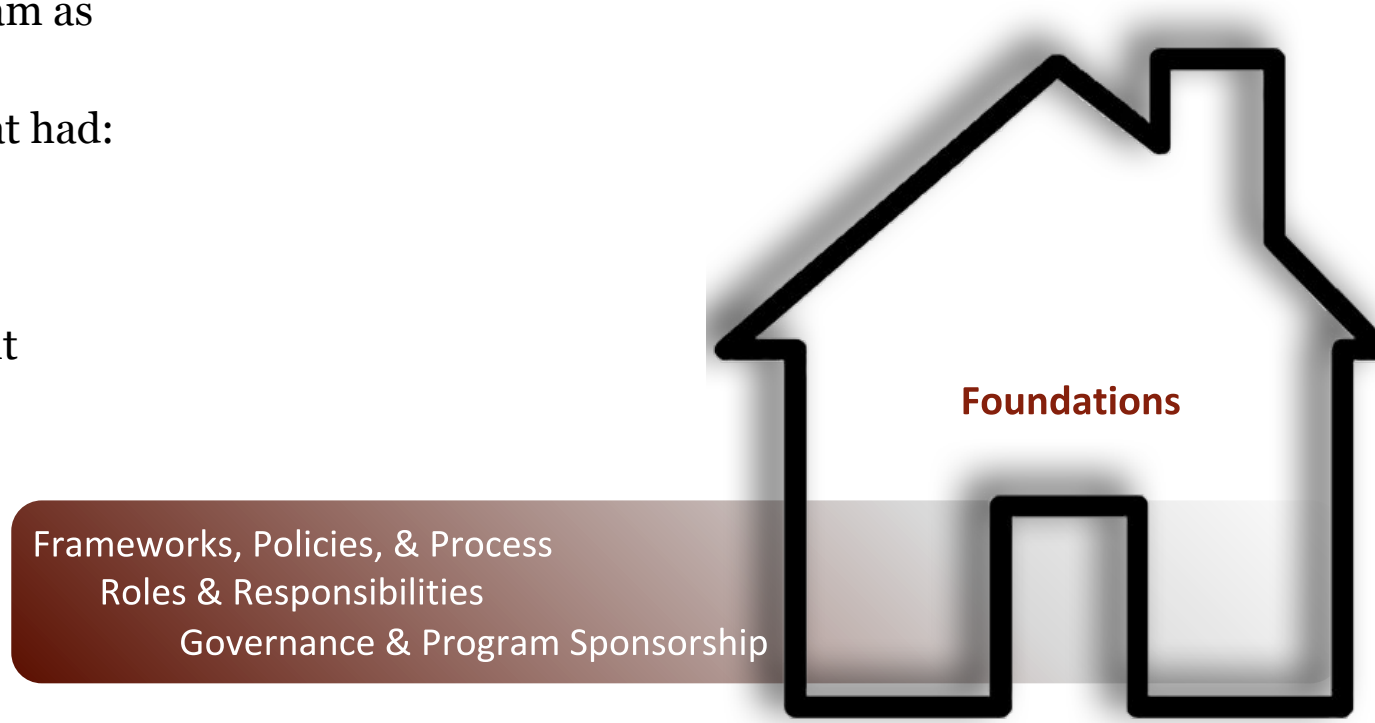
Components of a Solid TPRM Program

Foundations, Assessments, Operations



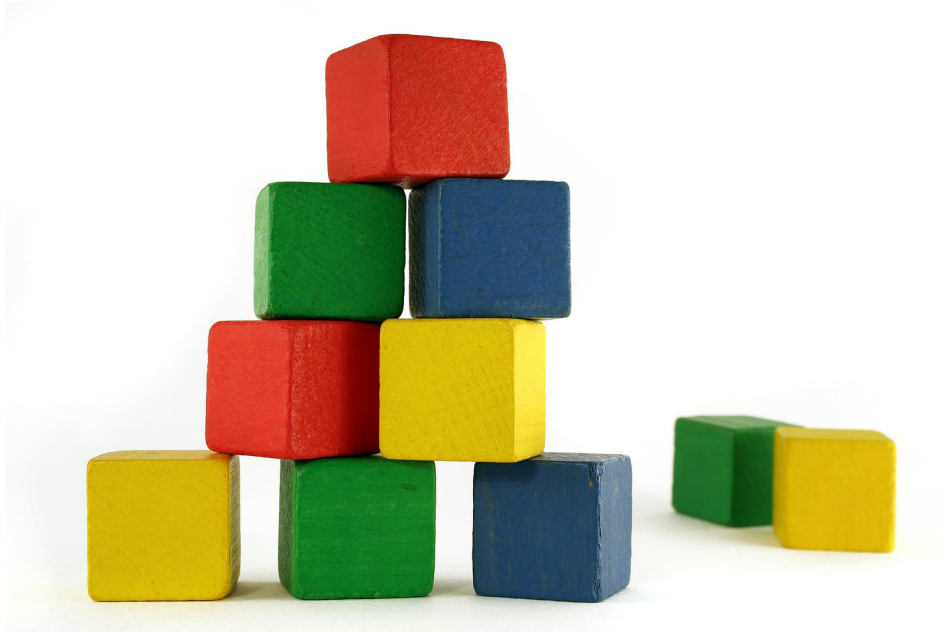
Stories from the Field: Roles & Responsibilities

- Case file:
  - Large company in the hospitality industry
  - 100s of third-parties: managing customers, managing properties, etc.
  - One IT administrator managed TPRM program as additional duty
  - New Director of Risk inherited a program that had:
    - No clearly defined mission
    - A skeleton budget and resources
    - No real metrics to report to management
- Lessons learned:
  - Symptom of lack of executive sponsorship
  - Tools alone don't substitute for governance



Program Considerations

- Governance
  - Program Drivers
  - Sponsor
  - Cross-functional participants
- Assessment Process
  - From Business to Cyber
  - Questionnaires / Frameworks
  - Interviews / Onsite Assessments / Evidence Gathering
  - Tools – Current / Planned
- Population
  - Number of vendors and other third parties
  - Tiering / Third Party Criticality



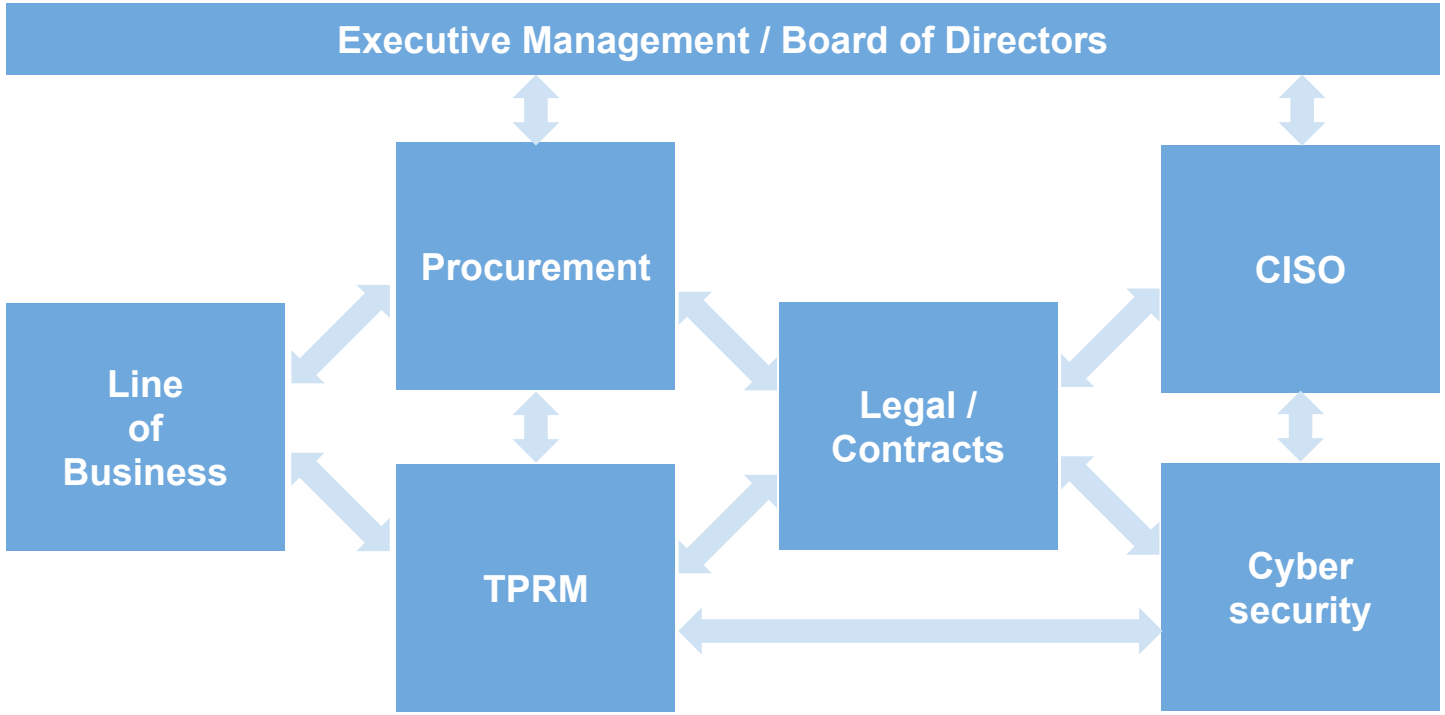
Stories from the Field: Align with Business Goals

- Case file:
  - What are the risk goals of the organization?
  - Are they well known across all areas of risk management?
  - In many cases, operations believes their role is to limit liability, not necessarily to reduce risk
- Lessons learned:
  - Need a clear vision, align with these objectives
  - Get buy in with from stakeholders / points-of-interaction
    - Executive management
    - Procurement--Enterprise and operating units
    - Lines-of-business
    - IT risk / cybersecurity

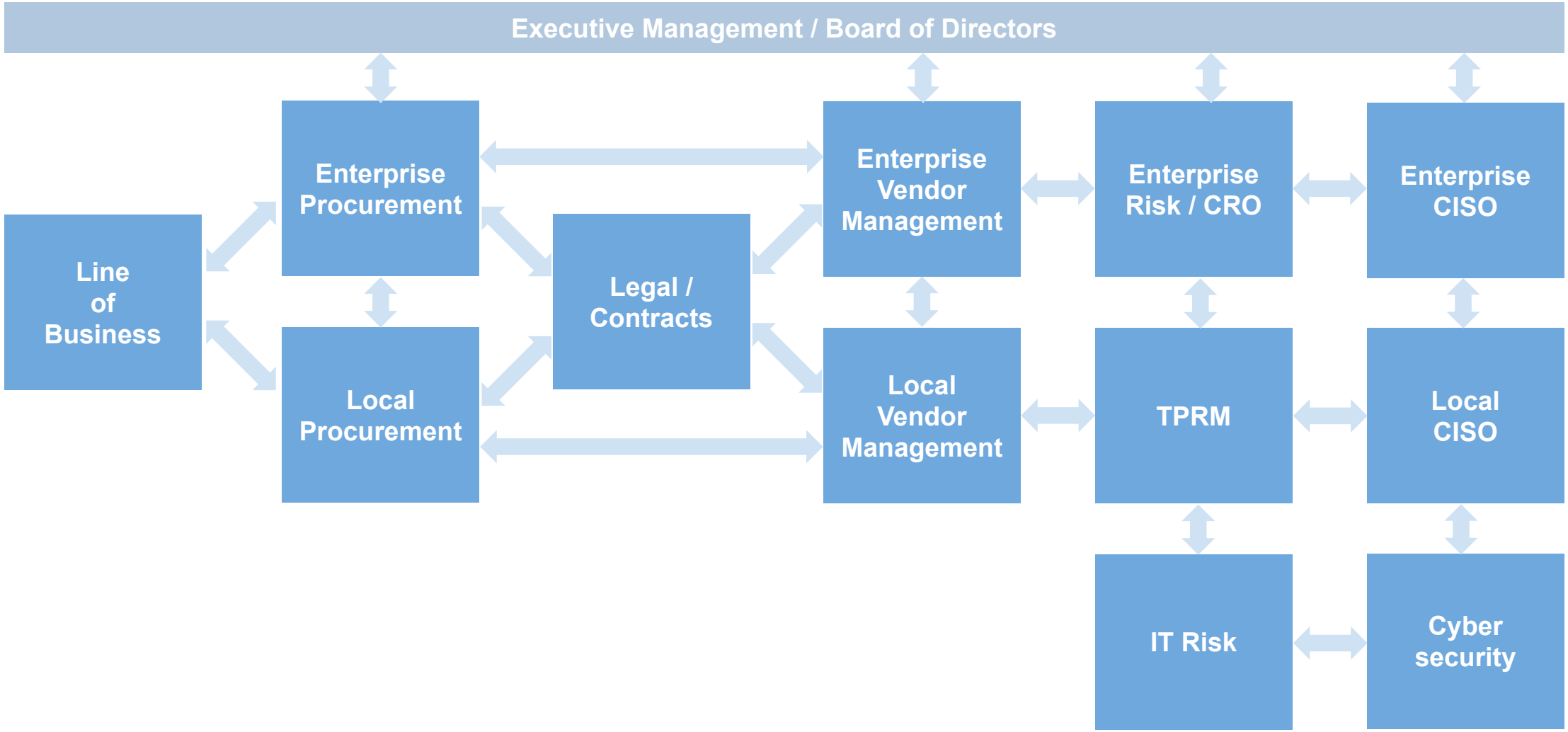
Stories From the Field: Know Your Organization's Personality

- Case file:
  - IT risk / cybersecurity only involved in vendor selection and assessment if LOB remembered
  - Sometimes procurement or legal flagged vendor, sometimes IT risk finds out about vendor after contract is signed
  - Culture of innovation, laissez-faire
- Lessons learned:
  - Culture can dictate decentralized decisions vs. top-down policy
  - Find the right checks and balances for your culture

Example Stakeholder Model (Medium Enterprise)



Example Stakeholder Model (Large Enterprise / Complex)



Stories From the Field: When in Doubt, Include IT Risk

- Case file
  - Well designed VRM and TPRM process
  - Strong support from management, central authority, published process
  - LOB ordered forklifts, which were not flagged as IT risks by LOB
  - Forklifts required IP addresses (everything is an IoT device), triggered late-stage cyber risk assessment
- Lessons learned
  - Involve IT Risk in all inherent risk assessment
  - Provide a feedback loop so vendor categories and goods/services are assigned a risk type that can be updated as products evolve

Stories from the Field: Stale Process

- Case file
  - Questionnaires rule, with SOC2, ISO, and other audit results / attestations by a nose
  - Lack of trust in actual data, which is more accurate and shows the ground truth
  - Fear of change, fear of becoming obsolete
- Lessons learned
  - Don’t be afraid to evolve your processes, that’s how you can optimize resources
  - There isn’t a trade-off between optimizing resources and reducing risk: you can have both
  - Plan for how to manage the message to existing staff; offer them enhanced roles

BITSIGHT®

Improving Questionnaires

Questionnaires

Framework-based Assessments / Questionnaires

Pros

- Align with sources of best practice (ISO, NIST, etc.)
- Clarify elements of policy
- Review program components not visible externally

Cons

- Difficult to verify and validate responses
- Process can be time-consuming
- Only represent a point in time

Selecting the Right Questions

- A question should help to determine the existence of a control that mitigates risk
  - Data Breach or Loss
  - Spread of malware
  - Potential sabotage (i.e. network interruption, disrupt “the grid”)
- Consider limiting questions about Policies, Processes and Security Assessment Reports (i.e. SOC2)
  - Instead create a ”Document Collection List”
  - Assume if a document is not submitted, it does not exist
  - Documents are generally clues to the existence of a control, not a control that mitigates risk

Streamlining Current Questionnaires

- Eliminate redundant questions

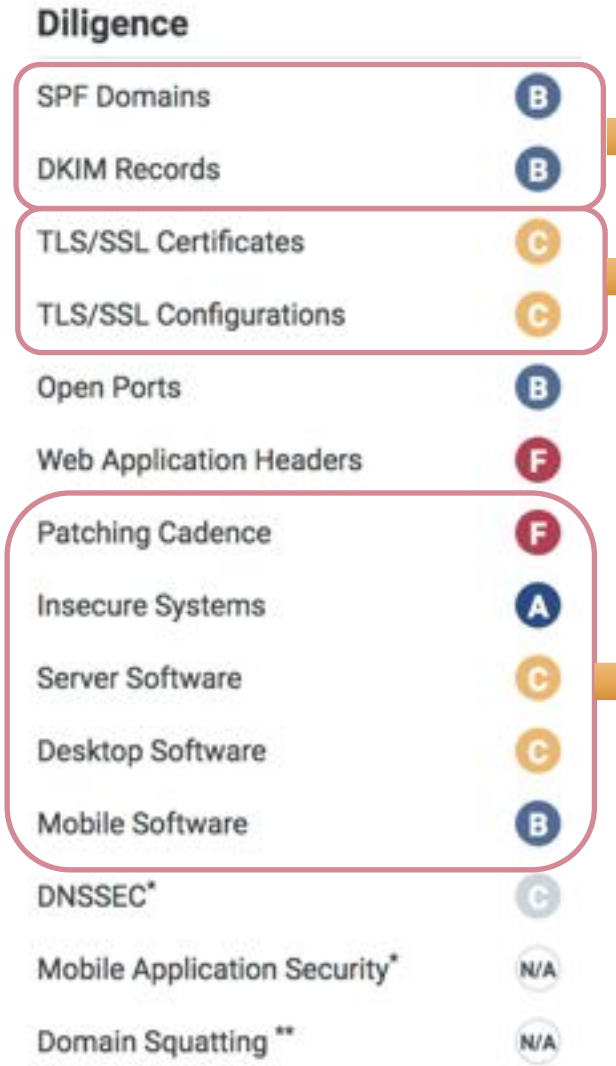
16	Has the management established an information security awareness and training program? If yes, please describe.

18	Are employees and contractors required to complete a security awareness training? If yes, please list the topics covered and the frequency of the information security training program, and specifically highlight whether users are trained to identify and prevent phishing attempts?

- Eliminate overly granular questions

Program must ensure that the destruction of a key is witnessed by the key custodians with the appropriate records retained for audit purposes. Each key or key component destruction should record the following:
- The date and time of the keying material destruction
- The reason for destroying the keying material
- The full name and signature of the individual authorizing the destruction
- The full name and signature of the individual destroying the keying material, and
- The full name and signature of the persons witnessing the destruction.

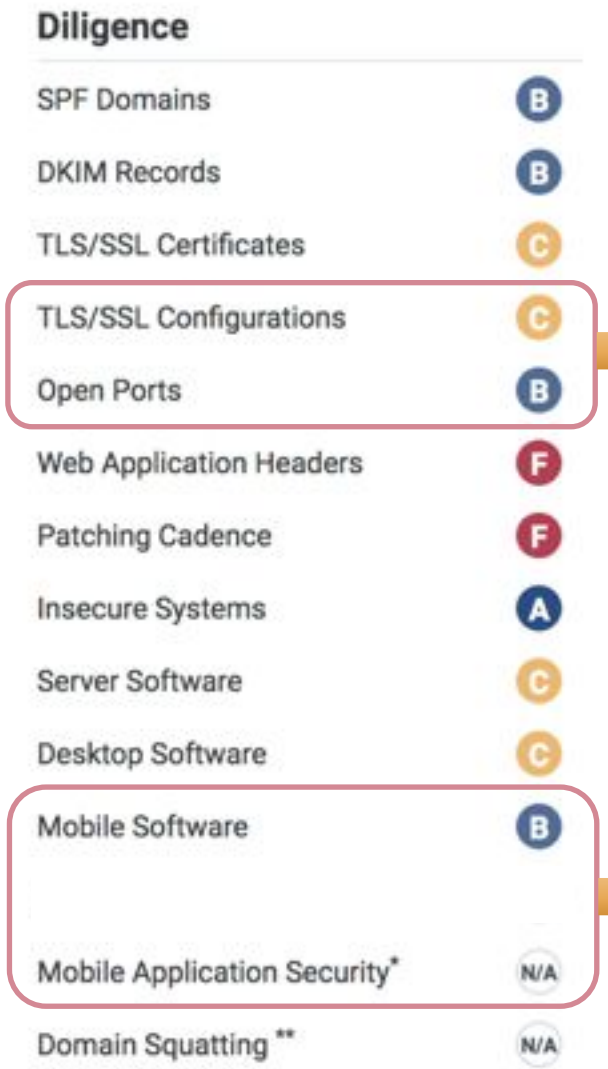
Aligning Questions with Risk Vectors



- Email security
- Encryption
- Vulnerability management
- Patch Management
- Configuration Management
- Hardening standards

What evidence do you have about security program practices?

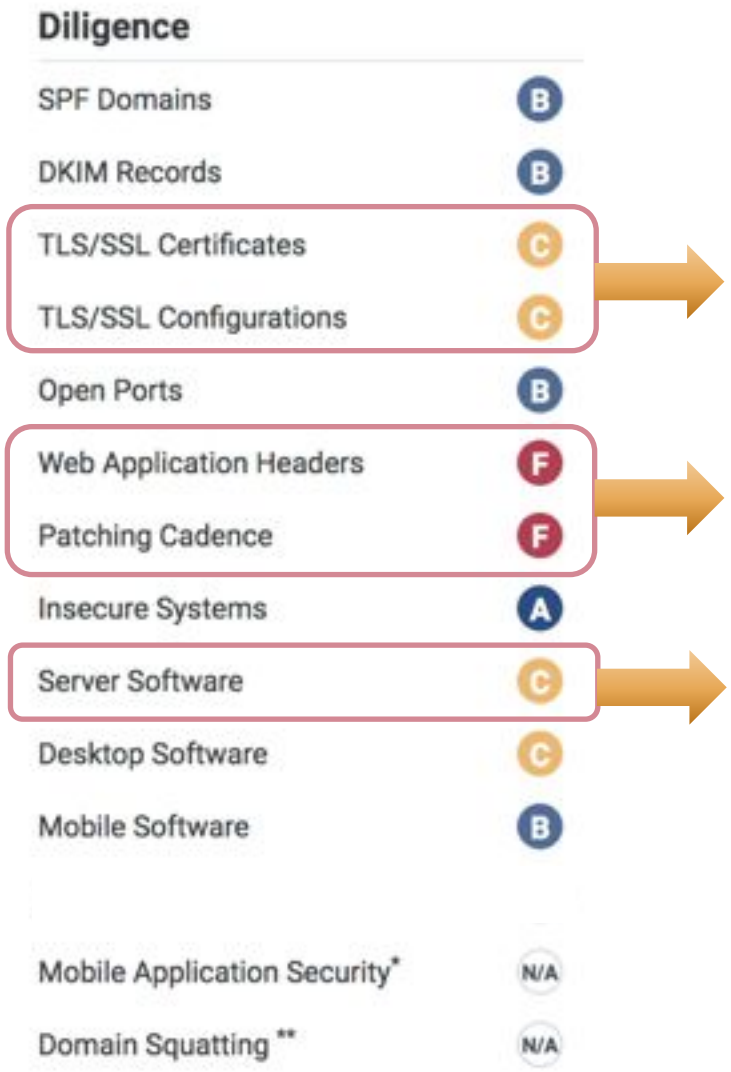
Aligning Questions with Risk Vectors



- Perimeter security
- PCI Compliance
- Firewall Standards

- Mobile security
- Secure development

Aligning Questions with Risk Vectors

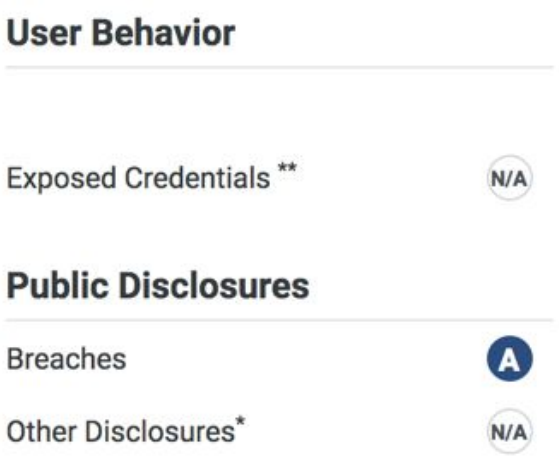


- Secure development (SDLC) / Web application security / [Sec]DevOps
- Encryption
- Config / change management

Aligning Questions with Risk Vectors

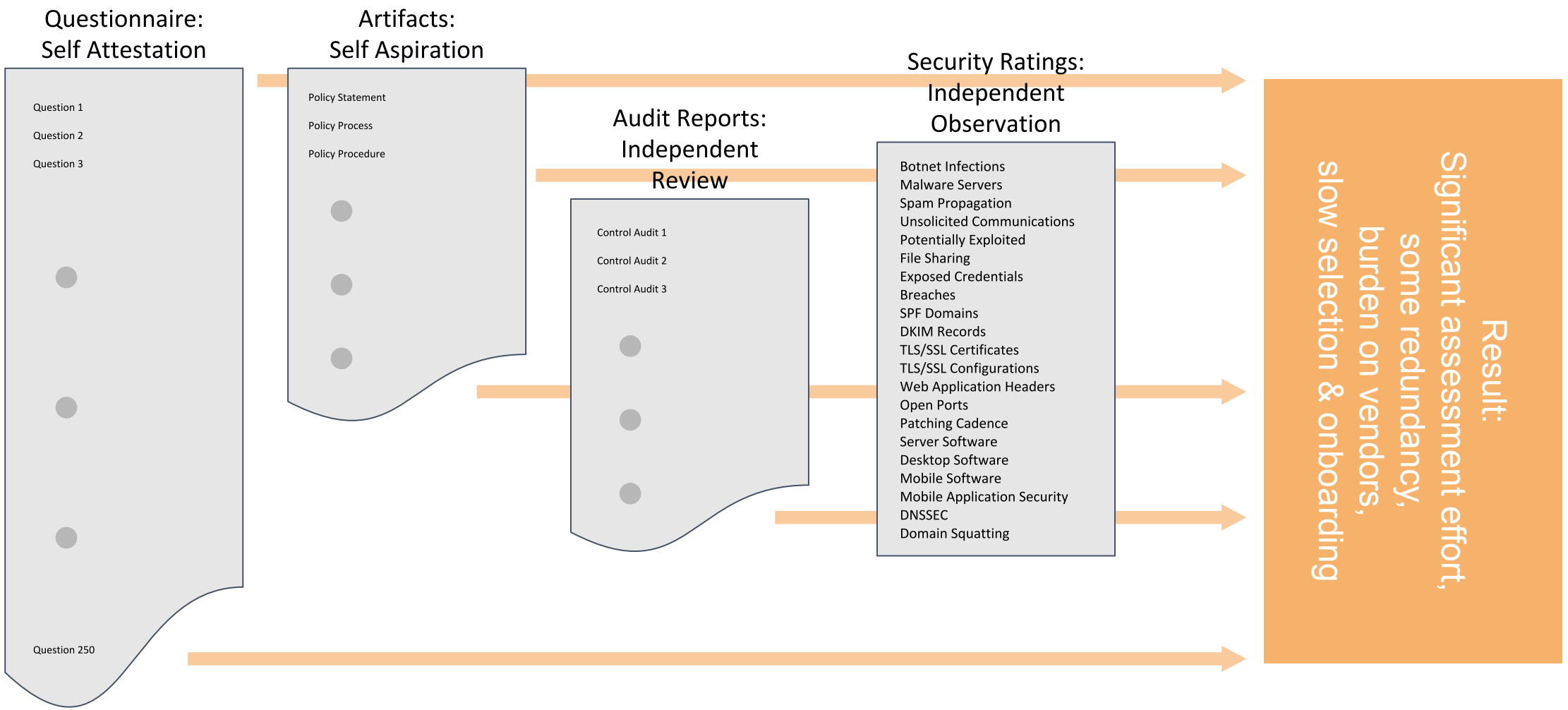
- Endpoint protection
- Incident management / Detection and response
- Security awareness / training

Aligning Questions with Risk Vectors



- Incident management
- Data loss prevention
- Secure disposal
- Capacity management / BCP

How It's Done Today



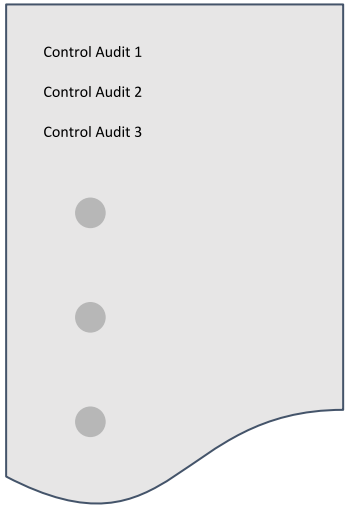
Modified Process: Less Effort, Less Risk

Security Ratings:
Independent
Observation

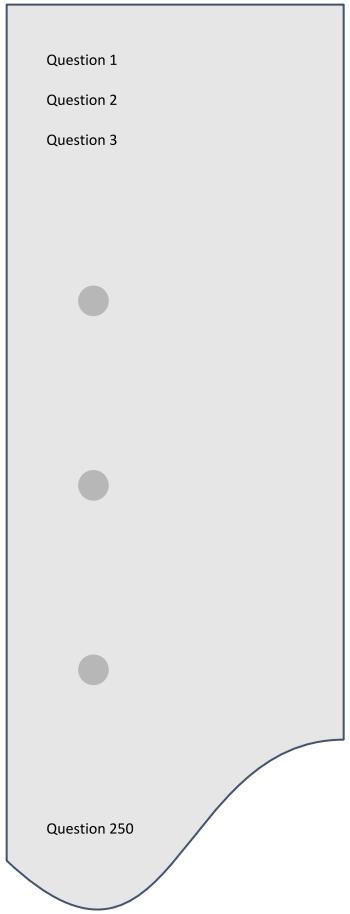
Botnet Infections
Malware Servers
Spam Propagation
Unsolicited Communications
Potentially Exploited
File Sharing
Exposed Credentials
Breaches
SPF Domains
DKIM Records
TLS/SSL Certificates
TLS/SSL Configurations
Web Application Headers
Open Ports
Patching Cadence
Server Software
Desktop Software
Mobile Software
Mobile Application Security
DNSSEC
Domain Squatting

Artifacts:
Self Aspiration

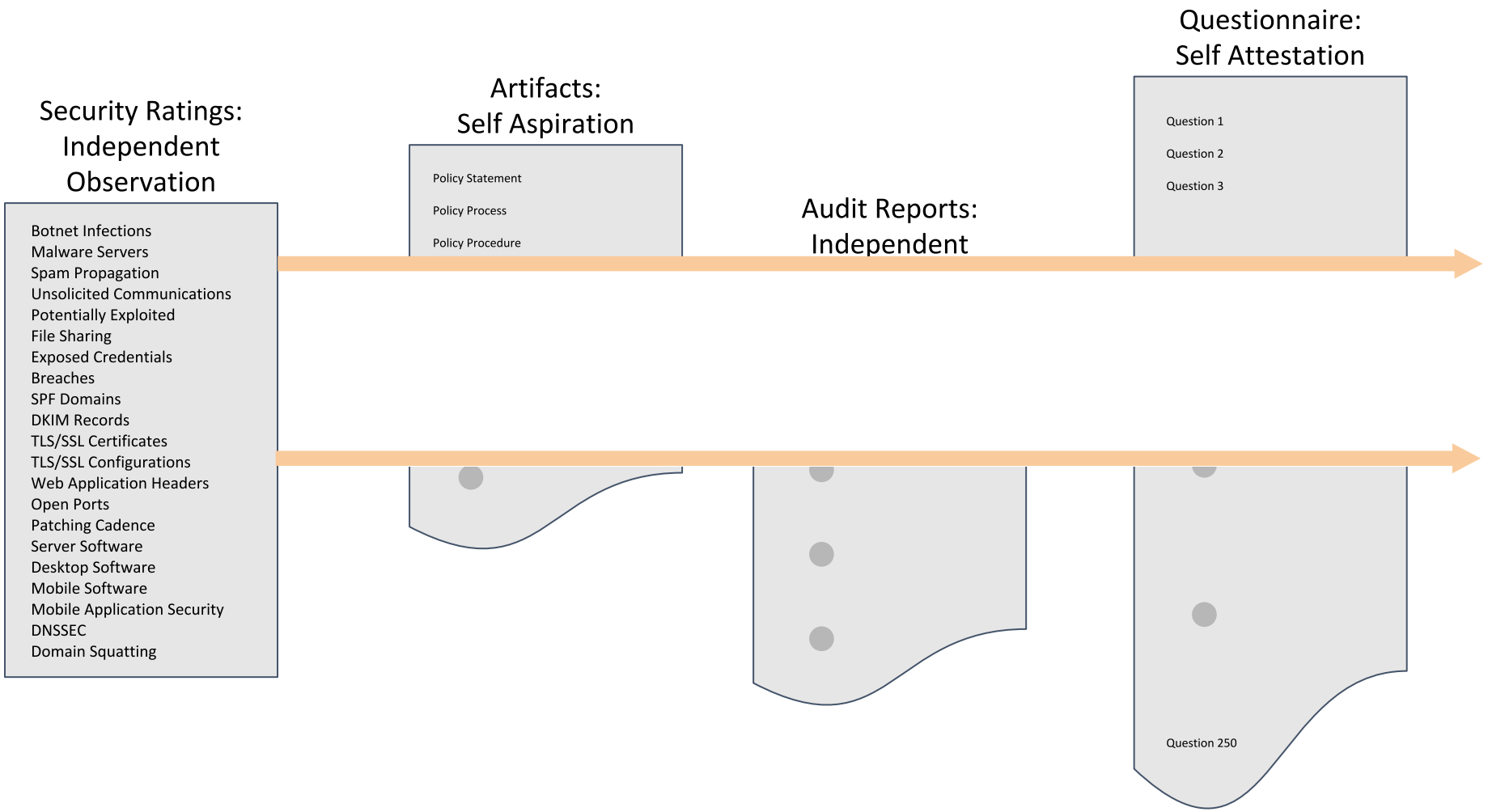
Audit Reports:
Independent
Review



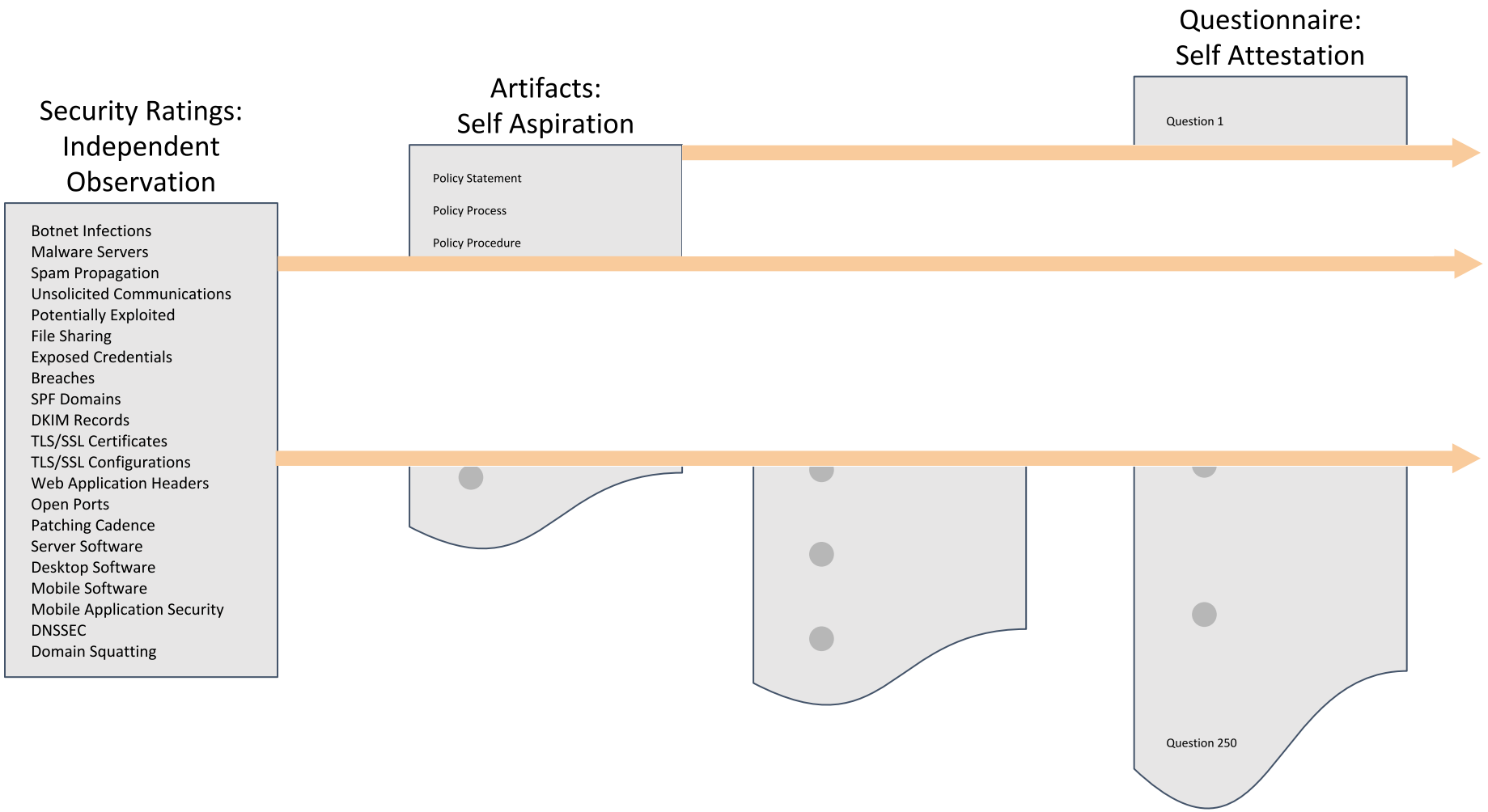
Questionnaire:
Self Attestation



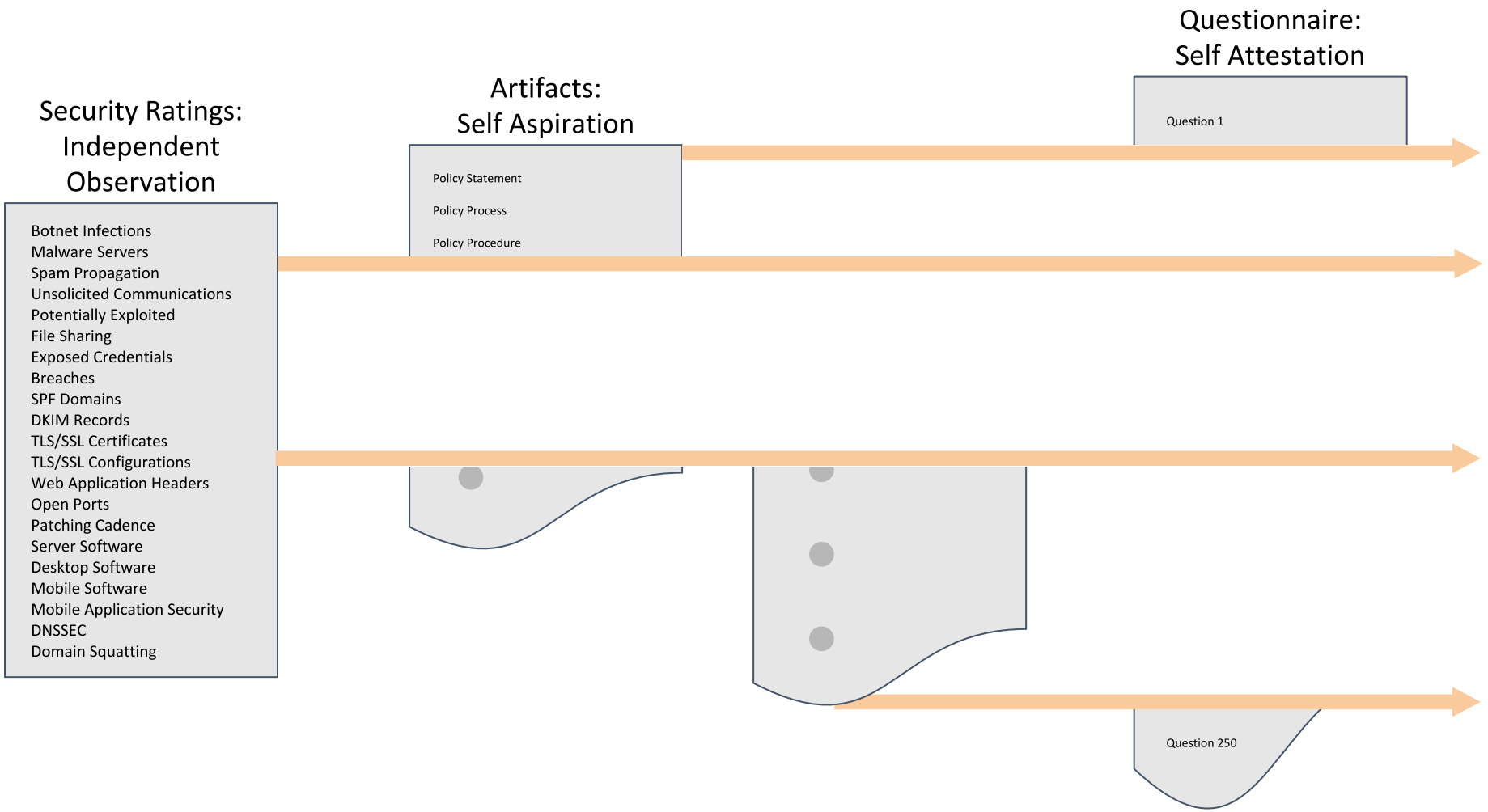
Modified Process: Less Effort, Less Risk



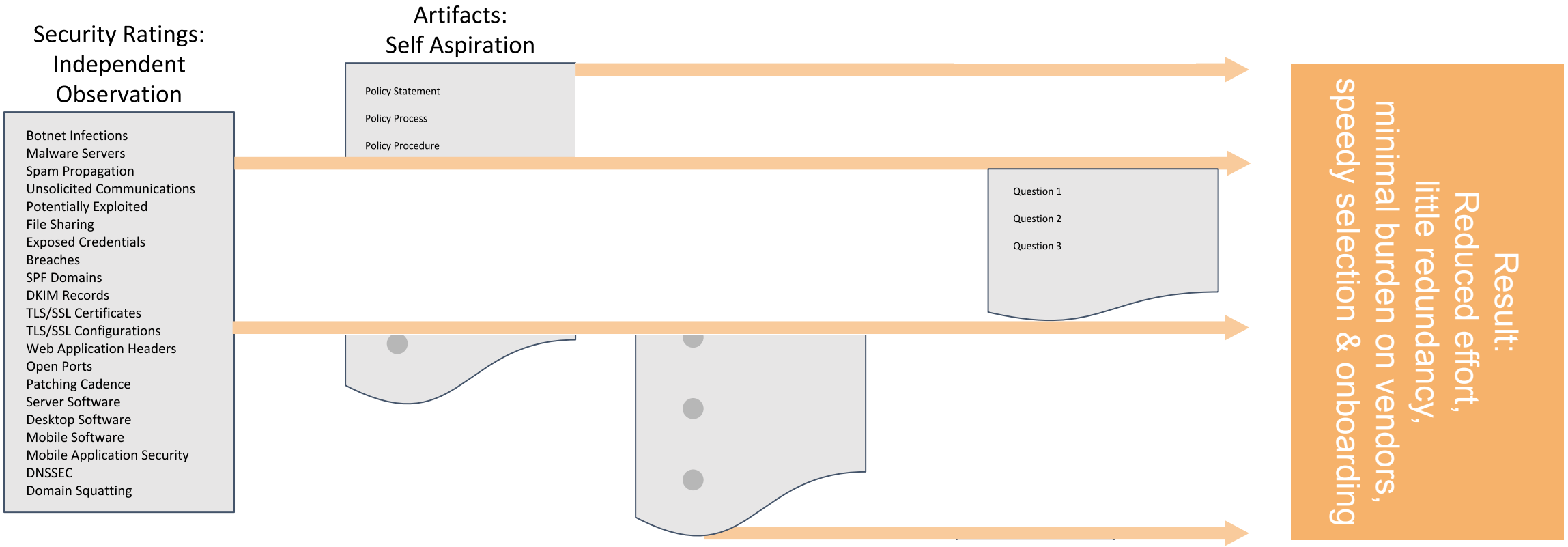
Modified Process: Less Effort, Less Risk



Modified Process: Less Effort, Less Risk



Modified Process: Less Effort, Less Risk



BITSIGHT®

Tiering and Vendor Communication

Third Party Tiering

- Business Risk
  - Nature of Services and Industry
  - Geography
  - Financial Strength / Credit Worthiness
- Data Criticality
  - Data Classification – Confidential, Sensitive, Proprietary or similar
  - Sensitive Data Types – PII, Customer Data, Compliance, other protected data
- Connectivity
  - Direct connections to network
  - Indirect connections or access

Vendor Communication

Leverage

…can we influence security improvements?

Context

…does it align with service the business uses?

Contract Clauses

Please note that the following does NOT constitute legal verbiage or advice from BitSight not any individual employed by or associated with BitSight.

<customer> will monitor <vendor> using a security rating system (SRS)

<vendor> will assign a point-of-contact for responding to inquires about the ratings observations.

<vendor> agrees to maintain a minimum rating and standards for each observation area (e.g., risk vectors), as follows: 650 or above for the overall rating, an A for Botnet Infections and File Sharing, and a B for Open Port and the remaining risk vectors that count toward the overall rating.

<vendor> agrees to investigate observations made by the SRS, explain the reasons for the observations, and cooperatively come up with an action plan to remedy negative observations.

<vendor> will work with the SRS platform to provide context, such as, but not limited to, breaking out assets that comprise the risk surface relevant to <customer>, tagging assets, and adding notes to observations

An Engaged Community Adds Context

PARTICIPANTS

CUSTOMERS - 1,700 TOTAL

1,700	2,063	100+
CUSTOMERS	EVA RECIPIENTS	PARTNERS

ACTIONS

5,541
EVAs Sent in the Last 12 Months

2,444
Self-Published Ratings

130,000+
Pieces of User Generated Content

OUTCOMES

More vendors familiar with BitSight ratings for better ***collaboration***

Gain insights from your vendors to better ***prioritize*** *follow up action*

Add context to ***communicate*** *your security posture with customers, regulators, insurers*

Prioritize issues with more ***context*** *than other ratings platforms*

BITSIGHT®

Process Optimization

Optimizing Assessment Resources

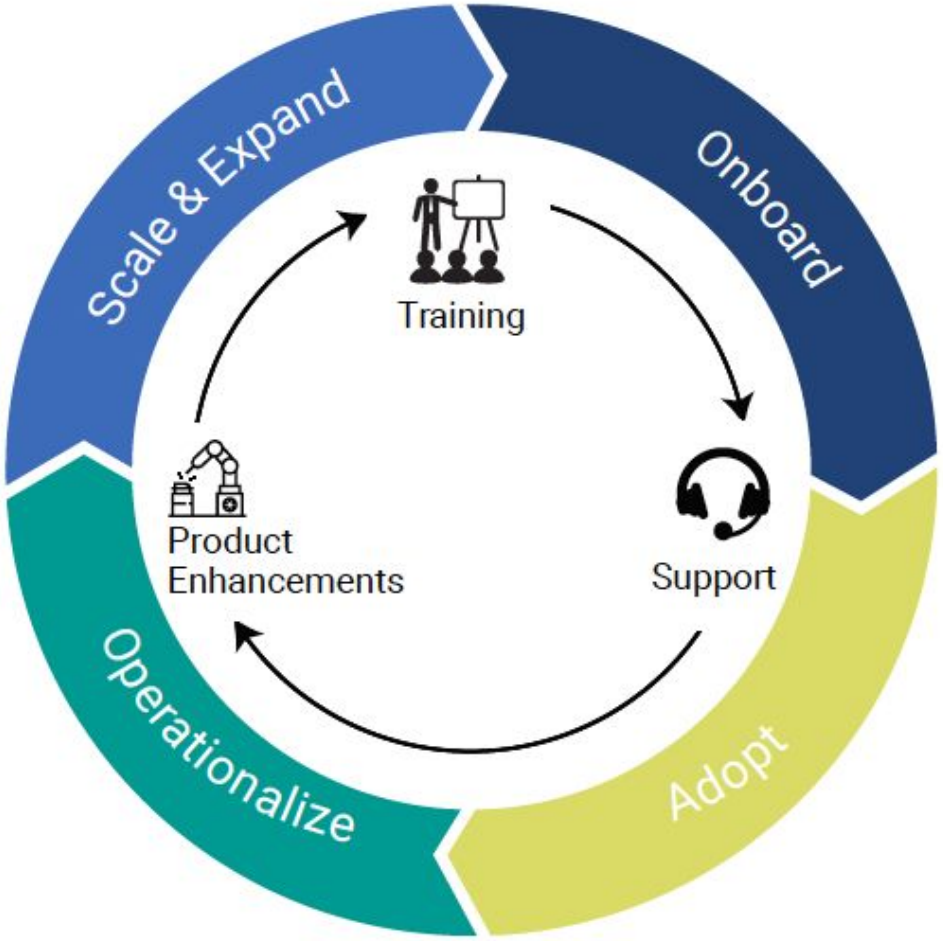
Initial Assessment / Onboarding			
	Tier 1	Tier 2	Tier 3
Rating >= 750 AND Botnet = A AND Open Ports > C AND File Sharing = A AND Breach = A	Partial questionnaire / assessment	Attestation (ISO, NIST, SOC)	Onboard (no assessment)
Rating 650-750	Full assessment	Partial assessment, focusing on gap areas	Attestation (ISO, NIST, SOC)
Rating 500-650 OR Botnet <=C OR Open Ports = F OR File Sharing <=C OR Breach >= C	Onsite audit	EVA outreach, possible onsite audit	Full assessment and EVA outreach
Rating < 500	Refuse vendor	Onsite audit	EVA outreach

Continuous Monitoring Action Matrix

Continuous Monitoring / Reassessment Period			
	Tier 1	Tier 2	Tier 3
Rating >= 750	Attestation (ISO, NIST, SOC)	No reassessment	No reassessment
Rating 650-750	Partial assessment, focusing on gap areas	Attestation (ISO, NIST, SOC)	No reassessment
Rating <650	Onsite audit	EVA outreach, possible onsite audit	Partial assessment, focusing on gap areas
Botnet <=B	EVA outreach	EVA outreach	EVA outreach
File Sharing <=B	EVA outreach	EVA outreach	EVA outreach
Open Ports = F	EVA outreach	EVA outreach	EVA outreach
Data Breach <C	Onsite audit	Onsite audit	Onsite audit
Data Breach A or B	EVA outreach	EVA outreach	EVA outreach

GRC tools, such as ServiceNow, and TPRM/VRM, such Whistic and Third Party Trust can automate and orchestrate risk management

Customer Success that's Part of Your Program



- *Your Customer Success Manager is a strategic partner that accelerates your time-to-value with proactive engagement, from onboarding to operationalizing and beyond.*
- *Your Customer Success Manager is your trusted advocate to ensure you realize maximum value with BitSight. They will guide and advise you on the development of strategic and tactical roadmaps, understand your long and short-term needs, advise you on new product features and help you achieve your objectives.*

Onboard

Implementation

- BitSight Training
- Tiering Vendors
- Alerts & Triage Process

Adopt

Enable Vendor Access (EVA)

Portfolio Reporting

- Quality & Rating Change Analysis

Integrations

- SAML
- API

Operationalize

Collaboration

- Tagging & Annotations
- User Working Groups
- Expansion of EVAs & Vendor Re-Assessment Process

Scale & Expand

Scaling up VRM Program

Full Vendor Lifecycle

- Selection
- Onboarding
- Monitoring

Automation driven action plans (through GRCs)

BITSIGHT

Questions

BITSIGHT

111 Huntington Ave, Suite 2010
Boston, MA 02199

info@bitsight.com